

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

---

In re Patent Application of:  
Siegried Keoppen et al.

Application No.: 10/563,337

Confirmation No.: 8841

Filed: January 3, 2006

Art Unit: 2431

For: METHOD FOR USE IN A NETWORK BASED  
SAFETY DATA STORAGE SYSTEM

Examiner: Sarah Su

**APPELLANTS' REPLY BRIEF ON APPEAL UNDER 37 C.F.R. § 41.41**

MS Appeal Brief-Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

March 26, 2010

Dear Sir:

Appellants submit this reply brief for the consideration of the Board of Patent Appeals and Interferences (the "Board") in response to the Examiner's Answer mailed February 3, 2010.

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is Deutsche Telekom AG. The inventors having assigned their rights in and to this application to Deutsche Telekom AG, such assignment having been duly recorded.

II. RELATED APPEALS AND INTERFERENCES

To appellants' knowledge, there are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

Claims canceled: 1;

Claims withdrawn from consideration but not canceled: none;

Claims pending: 2-16;

Claims allowed: none;

Claims rejected: 2-16.

**Claims on Appeal**

The claims on appeal are 2-16.

IV. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1) Whether claims 2-10 and 13 can properly be rejected as obvious under 35 U.S.C. § 103(a) based on a combination of U.S. Published Application No. 2004/0054750 to de Jong et al. ("de Jong") and U.S. Published Application No. 2003/0174842 to Challenger.

2) Whether claims 14-16 can properly be rejected as obvious under 35 U.S.C. § 103(a) based on a combination of de Jong, Challener, and U.S. Patent No. 5,901,227 to Perlman.

3) Whether claims 11-12 can properly be rejected as obvious under 35 U.S.C. § 103(a) based on a combination of de Jong, Challener, and U.S. Published Application No. 2004/0010715 to Winiger et al. ("Winiger").

V. ARGUMENTS IN RESPONSE TO EXAMINER'S ANSWER MAILED FEBRUARY 3, 2010

The assertions set forth in the Appeal Brief filed November 5, 2009 are respectfully maintained. The following points are made to clarify those assertions and answer any new contentions set forth in the Examiner's Answer dated February 3, 2010.

Grounds of Rejection No. 1: Obviousness rejection of claims 2-10 and 13 based on a combination of de Jong and Challener

It is respectfully submitted that a combination of de Jong and Challener would not render claims 2-10 and 13 obvious.

Independent claim 2 of the present application is directed to a method for data storage on a server in a telecommunications network. Claim 2 recites setting up a personal main folder on the server for a first user and configuring the personal main folder to have a functional locker that provides "a personal locker, wherein a reference to first files of the first user is storable in the personal locker only by the first user and displayable only to the first user."

In the Examiner's answer of February 3, 2003, the Office asserts that de Jong discloses that a content producer provides digital content to at least one content repository and a description of the content to at least one content provisioner (that is, a personal locker, according to the Office) and that the description of the digital content may comprise a URL, part of a URL, a summary of the digital content, a hash of the digital content, or the like, and that since the description of the digital

content has been described as a link for the content, the description has been interpreted by the Office as a reference to the content. *See* Examiner's Answer, p. 18, lines 12-19.

It is respectfully submitted that de Jong does not teach or suggest that a user stores content or a reference to the content. In the Examiner's Answer, it appears that the Office is equating a user and a content producer. Applicants submit that there is a clear distinction in de Jong between the user 2702 (*i.e.*, one who issues an access request) and the content producer 2710 (*i.e.*, a system component that stores digital content or a reference to the digital content). Content producer 2710 of de Jong provides digital content to a content repository 2708, and provides a description of the content to a content provisioner 2724. *See* De Jong, ¶¶ 0174-175; Fig. 27. The de Jong user 2702 merely issues an access request to the particular content producer, using a mobile phone 125-140, so as to access digital content stored by a content producer 105-120. *See* De Jong, ¶¶ 007-08; Fig. 1. Therefore, the user of de Jong may access but does not store content or a reference to the content, as required by claim 2.

It is further respectfully submitted that de Jong does not teach, or suggest, a personal locker that contains references to files of a first user that are displayable only to that first user, as required by claim 2. In contrast, de Jong merely describes a system that includes content database 340 or content repository 2708 that contains digital content provided by content producer 2710. *See* De Jong, ¶¶ 0174; Fig. 27. De Jong does not teach, disclose or suggest that the content storer is the only user to which a reference to the content is displayable, as required by claim 2. Even if the use of a token makes the digital content only available to one user, as asserted in the Examiner's Answer (*See* Examiner's Answer, p. 19, lines 5-8), and which it is respectfully submitted is not the case, the user 2702 of de Jong still stores no reference to the file of the user, as required by claim 2.

It is respectfully submitted that Challenger fails to cure the deficiencies of de Jong with respect to the recited features of independent claim 2. Accordingly, a combination of de Jong and Challenger, to the extent proper, could not render independent claim 2, nor dependent claims 3-10 and 13, obvious.

Grounds of Rejection No. 2: Obviousness rejection of claims 14-16 based on a combination of de Jong, Challener, and Perlman

Claims 14-16 depend from independent claim 2, and recite the features of claim 2 as if set forth therein. Appellants respectfully submit that Perlman does not cure the deficiencies of de Jong and Challener in that Perlman does not teach the features of claim 2 of setting up a personal main folder on the server for a first user and configuring the personal main folder to have a functional locker that provides “a personal locker, wherein a reference to first files of the first user is storable in the personal locker only by the first user and displayable only to the first user.” Because claims 14-16 depend from claim 2, a combination of de Jong, Challener and Perlman, to the extent proper, could not render dependent claims 14-16, obvious.

Grounds of Rejection No. 3: Obviousness rejection of claims 11 and 12 based on a combination of de Jong, Challener, and Winiger

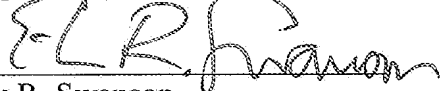
Claims 11-12 depend from independent claim 2, and recite the features of claim 2 as if set forth therein. Appellants respectfully submit that Winiger does not cure the deficiencies of de Jong and Challener in that Winiger does not teach the features of claim 2 of setting up a personal main folder on the server for a first user and configuring the personal main folder to have a functional locker that provides “a personal locker, wherein a reference to first files of the first user is storable in the personal locker only by the first user and displayable only to the first user.” Because claims 11 and 12 depend from claim 2, a combination of de Jong, Challener and Winiger, to the extent proper, could not render dependent claims 11 and 12, obvious.

**CONCLUSION**

For all of the reasons set forth above, it is respectfully submitted that the rejections of claims 2-16 should be reversed. Appellants respectfully request that the rejections be withdrawn, and the case passed to allowance.

Dated: March 26, 2010

Respectfully submitted,

By 

Erik R. Swanson

Registration No.: 40,833

DARBY & DARBY P.C.

P.O. Box 770

Church Street Station

New York, New York 10008-0770

(212) 527-7700

(212) 527-7701 (Fax)

Attorney For Applicant(s)

**APPENDICES**

**CLAIMS APPENDIX**

The following is a copy of the claims involved in the appeal:

Claim 1 (Canceled)

Claim 2 (Previously presented): A method for data storage on a server in a telecommunications network, the telecommunications network providing connectivity between local computers of users and the server, the method comprising:

issuing, upon request, by an operator of the server, to a first user of the users a user certificate for access conditions;

providing the user certificate and a secret key to the first user;

accessing the server over an internet;

sending, by the server, a client program to a first local computer of the first user, the client program enabling an authentication of the first user using the user certificate and a transmission of at least one further security requirement;

setting up a personal main folder on the server for the first user, the main folder having a first special file including a first security requirement defined for the main folder and first management information so as to provide a main locker;

configuring the personal main folder to have at least one further folder set up therein, the at least one further folder having a function and a second file including a second security requirement defined for the least one further folder and including second management information so as to provide a functional locker;

displaying the functional locker only if at least one security-relevant requirement is met so as to provide a locker system having a virtual character, wherein the functional locker provides a personal locker, wherein a reference to first files of the first user is storable in the personal locker only by the first user and displayable only to the first user, and at least one of:

a provisioning locker, wherein a first reference to a different second file available to another user is storable therein only by the first user; and

a receiving locker, wherein a third file of a second user of the users is storable therein only by the second user, the receiving locker being configured, when opened, to provide to the first user a sender user reference relating to the storage of the third file and to a sender user defined security requirement.

Claim 3 (Previously presented): The method as recited in claim 2 wherein the certificate includes a public key.

Claim 4 (Previously presented): The method as recited in claim 2 further comprising providing a public key to the first user.

Claim 5 (Previously presented): The method as recited in claim 2 wherein the providing the user certificate and the secret key to the first user is performed by providing the user certificate and the secret key on a smart card.

Claim 6 (Previously presented): The method as recited in claim 2 wherein the at least one further security requirement includes at least one of a biometric system requirement, a geographic positioning requirement, a time restriction, a network requirement, and a computer data requirement.

Claim 7 (Previously presented): The method as recited in claim 6 wherein the at least one further security requirement includes a time dependency.

Claim 8 (Previously presented): The method as recited in claim 2 wherein the at least one further security requirement is a requirement of at least one of the operator of the server, the first user, and a sender of the third file.



Claim 9 (Previously presented): The method as recited in claim 2 wherein the provisioning locker has a name associated therewith.

Claim 10 (Previously presented): The method as recited in claim 2 wherein the provisioning locker includes a user locker for the another user.

Claim 11 (Previously presented): The method as recited in claim 2 wherein the receiving locker has a name associated with a sender of the third file.

Claim 12 (Previously presented): The method as recited in claim 2 wherein the receiving locker includes a user locker for the sender user.

Claim 13 (Previously presented): The method as recited in claim 2 wherein the first user and the second user are each registered with the server, and further including the steps of:

- setting up a second personal main folder on the server for the second user, the second main folder having a respective first special file including a respective first security requirement defined for the respective main folder and respective management information so as to provide a respective locker,

- configuring each respective main folder to have respective further folders set up therein, the respective further folders each having a respective function and each having a respective second file including a respective second security requirement defined for the respective further folders and including the respective management information, each of the further folders acting as a respective functional locker,

- displaying each functional locker only if a respective security-relevant requirement is met, so as to provide a respective locker system having a virtual character, each functional locker providing a respective function of at least one of:

- a respective personal locker, respective first files being storable in the respective personal locker only by the respective user and displayable only to the respective user;

a respective provisioning locker, wherein a respective first reference to a respective second file for a different user being storable by the respective user therein;

a respective receiving locker for a respective third file available to a respective sender user of the users, the respective receiving locker being configured, when opened, to provide to the respective user a respective sender user reference relating to the storage of the respective third file and to a respective sender user defined security requirement; and

a respective public locker configured to store, by the first user, the first reference to the second file when the first reference is stored in the provisioning locker, if access to the first reference is offered to a plurality of different users.

Claim 14 (Previously presented): The method as recited in claim 2 further including the steps of:

storing a fourth file in the functional locker only if the second security requirement is met;

generating a random number from data of the fourth file so as to provide an access key;

encrypting the data using the access key;

subsequently encrypting the access key with a public key and then destroying the access key so that the access key, for accessing the stored file, can only be recovered using the secret key;

receiving, at the server, the encrypted data, a fourth management information of the fourth file, and the encrypted access key;

encrypting, by the server, the transmitted encrypted data a second time;

generating a unique file identifier for the fourth file;

storing the fourth file in a system locker using the unique file identifier; and

storing a fourth reference to the fourth file in the functional locker, the fourth reference including the unique file identifier, the encrypted access key, and the fourth management information.

Claim 15 (Previously presented): The method as recited in claim 14 wherein the functional locker is the provisioning locker including a user file for the other user, and further including the steps of:

enabling the stored fourth file to be forwarded by the first user to the other user only if the first user decrypts the encrypted access key with the secret key and re-encrypts the decrypted access key with a second public key of the other user, and

storing the re-encrypted access key, the file unique identifier and the fourth management information, as the fourth reference to the file into the user locker.

Claim 16 (Previously presented): The method as recited in claim 14, wherein the second management information includes a management requirement, and wherein the storing the fourth file is performed only if the management requirement is met.

**EVIDENCE APPENDIX**

None.

**RELATED PROCEEDINGS APPENDIX**

There are no related proceedings for this matter.